ACEEE

Int. J. on Recent Trends in Engineering and Technology, Vol. 10, No. 1, Jan 2014

Security for Future Networks: A Prospective Study of AAIs

H. Aissaoui-Mehrez[1], P. Urien[1], G. Pujolle[2], J. da Silva Fraga[3] and D. da Silva Böger[3]
[1]IMT-TELECOM-ParisTech: LTCI CNRS Laboratory : 46, rue Barrault 75634 Paris France
Email: {hassane.aissaoui, pascal.urien}@telecom-paristech.fr
[2]CNRS, LIP6/UPMC Laboratory,University Pierre and Marie Curie 4 Place Jussieu, 75005 Paris, France
Email: guy.pujolle@lip6.fr
[3]Centro Tecnológico, Departamento de Engenharia Elétrica : UFSC C.P. : 476 88040-900-Florianopolis,SC Brasil
Email: fraga@lcmi.ufsc.br,dsboger@gmail.com

***Abstract*— The future Internet will rely heavily on virtualization and Cloud networking. The project Security for Future Networks (SecFuNet)[1] proposes the design of a framework providing secure identification and authentication, secure data transfer and secure virtualized infrastructure.**

In this paper, we present some of the most important ones currently available and we present a comparative study should examine some models and frameworks of Identity Management. Initially, we had identified OpenID, Higgins and Shibboleth frameworks as those providing facilities that are the closest to our proposals and our requirements. However, with the literature prospection more frameworks have being included in our study, which has allowed to expand our state of the art on IdM. In our study, some features are highlighted and related with our objectives.

***Index Terms*— Microcontrollers, Single Sign-on, Security, Identity User-Centric, Virtualization, Cloud Networking.**

I. INTRODUCTION

The SecFuNet project proposes solutions for integrating secure microcontrollers in a global and secure Identity Management (IdM). The IdM system will be based on several local authentication servers composed by secure microcontrollers. Initially, some requirements were defined to this project; such as User-Centric and Federated Identities approaches for the IdM. The federated identities IdM deliver defined policies for releasing user attributes that often threaten user privacy. It occurs mainly because the idea of federations is centered on information sharing.

The objective is prospective and comparative studies examine some models and frameworks of IdM illuminated by the main concerns and requeriments of the SecFuNet Project.

The rest of this paper is structured as follows. The related work of the main concepts and approaches to IdM models are described in Section II. Section III, describes what Level of Assurance means and which factors affect this parameter. Next, Section IV an overview of the main infrastructures supporting these models, Section V compares different solutions of IdM models. In Section VI, we conclude with an overall description of first choice of solutions that will be used in this project and the benefits provided both to users and SPs, when identity and User-Centric models are used in IdM.

DOI: 01.IJRTET.10.1.1448

[1] SecFuNet : http://www.secfunet.eu/index.php/publications

II. RELATED WORK

The identity may be considered as a combination of sub-sets of so called partial identities, some of which uniquely identify a person and others not. Depending on the context and situation, a person may be represented by different partial identities. Within a company, the identity can be associated with roles, privileges, rights and responsibilities. It should be noted that the same personal information may be present in different partial identities of the user. An IdM is used to manage partial identities in a digital world, to ensure the entity associated to this digital identity and also, for delivering authenticated information contained in the corresponding identity [1].

A. Identity Management

An IdM integrates identities, attributes and policies, resulting in mechanisms for authenticating users and delivering attributes for business processes. Usually, an IdM is decomposed in the following elements [2]:

- ✓ User and Identity (Id) - are intimately linked. The user is the consumer of a service. The Id is a set of attributes that characterizes the user into a digital world. It can be his name, address, affiliation, etc.
- ✓ Identity Provider (IdP) - maintain the users directory of identifiers associated to users. After an authentication process, the user receives an assertion, that recognizing him in the domain of this IdP.
- ✓ Service Provider (SP) - provides resources to users after verifying its authenticity. Nevertheless, the SP may also demand some special user attributes what characterizes attributes based access controls (BAC).

B. Identity Management Models

IdM systems models are classified as conventional, centralized, federated and user-centered. The "Fig. 1" illustrates each model and their interactions in authentication procedures.

- *The conventional model* – the identities are individually handled by each SP, playing also the role of an IdP. Usually, user Ids are not shared among different SPs and this approach tends to be costly for both users and SPs. Each SP may require its own set of user attributes. For users, managing multiple identities is somewhat costly. The tedious task to provide the same information to create of their account in each SP may cause a careless or an inaccurate. In filling asked attributes that can be crucial to access the resource.
- *The centralized model* – appeared as an alternative solution to the inflexibility of the conventional model. It is based on the sharing of user identities between SPs and on the concept of Single Sign-on (SSO). In the centralized model, all SPs that have trust relationships with an IdP. The IdP is responsible for authenticating users and supplying user's attribute to SPs. The concept of SSO represents a great convenience to users since they only need perform the authentication process once and thereafter they can use the obtained credentials on all SPs they wish to access, until these credentials expire. The weak point of the centralized model is that the provider identity has absolute control over the information of its users [3].
- *The federated model* – In order to avoid the deficiencies presented by the centralized model, the federated identity model was introduced based on the distribution of the task of user authentication across multiple IdPs. These IdPs are arranged in different administrative domains IdP. This concept relies on trust relationships which are established among multiple IdPs and SPs and which optimizes information exchanges in user authentications [4]. The benefit is that it can handle a smaller number of users' information.
- *The User-Centric model* – aims to give the user full control over its digital identities, but the main implementations of this model are built around the previous models. However, this approach is most widely used with the federated model. The identities of a user are stored on a physical device which is held by the user, such as a smartcard or a cell phone. The user authenticates him in this device and may choose what identity he wants to use with a specific SPs. This approach fully respects privacy preferences of the user.

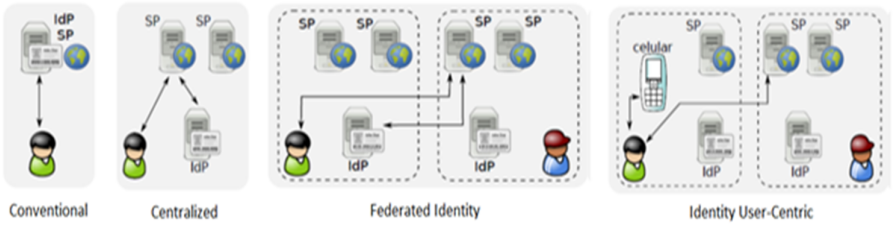

Figure 1. Identity Management Models.

III. LEVELS OF ASSURANCE

The U.S. National Institute of Standards and Technology (NIST) has released a guide on authentication process which defines four Levels of Assurance (LoA) . Level 1 is considered the weakest and the level 4 is the most robust. The corresponding documentation indicates the technical requirements for each level summarized, in figures below. “Fig. 2” shows the different kinds of tokens that may be used at each authentication assurance level. “Fig. 3” identifies the types of authentication protocols that are applicable to each assurance level.

Token type	Level 1	Level 2	Level 3	Level 4
Hard crypto token	√	√	√	√
One-time password device	√	√	√	
Soft crypto token	√	√	√	
Passwords & PINs	√	√		

Figure 2. LoA allocated to each Token Types

Protocol Type	Level 1	Level 2	Level 3	Level 4
Private key PoP	√	√	√	√
Symmetric key PoP	√	√	√	√
Tunneled or Zero knowledge password	√	√		
Challenge-response password	√			

Figure 3. Authentication Protocol Types

For example, an authentication process that makes use of user name and password is considered less robust than a process that makes use of hardware device that contains a protected cryptographic key. SPs could use these levels to provide different levels of authentication and authorization.

IV. AN OVERVIEW OF THE MAIN AAIS

A. SAML : Security Assertion Markup Language

SAML define a protocol for securely exchanging identity information: authentication, authorization and attributes, among applications regardless of the technologies used by each application (PKI, SSO, LDAP, Kerberos, etc.). The current version SAML (2.0) extends the former infrastructure with concepts and mechanisms derived from other projects (ID-FF V1.2: Liberty Alliance Identity Federation Framework) and Shibboleth V1.2 of Internet2 Consortium that have broader goals.

✓ *Secure exchange of the identity information*: SAML Core is an XML grammar for representing security information in assertion formats. In “Fig. 4”, SAML specifications define five components [5]: *The roles* that each entity can play in SAML infrastructure and the metadata describe these entities in this architecture. *The Profiles* describe the protocols and assertions to specific data transfers and single authentications. *The Assertions* specify the format to represent security information about a subject. *The Protocols* are used to request and transfer assertions between entities. *The Transport* consists of specifications defining how to use the underlying protocols (SOAP, HTTP, etc.) to transport these SAML messages.

✓ *Privacy in SAML and Federations:* SAML 2.0 provides support to the use of pseudonyms, which are dynamic identifiers and not related to the identity attributes of the subject. Pseudonyms serve as identifiers shared between SP and IdP and can be used in two ways:

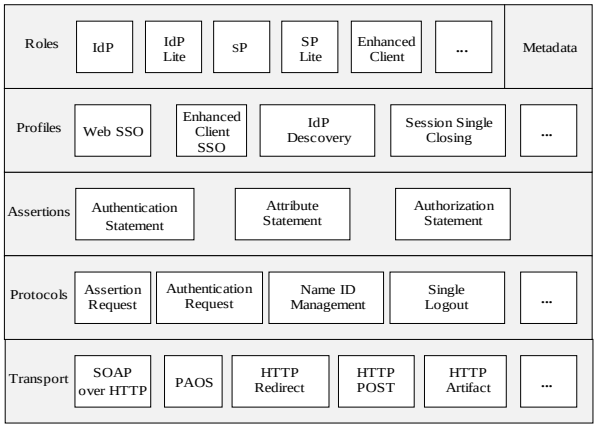

Figure 4. Components of SAML Specifications

- *The persistent pseudonym* is created once at the IdP and associated permanently to a subject identity. This scheme, combined with the privacy policies on access to subject attributes, can guarantee identity protection. However, access to different SPs can still be tracked if these SPs act in collusion.

- *The transient pseudonym* is created by the IdP and associated with the identity of a subject for the duration of the user session. Thus, the SP can still decide the subject access based on attributes issued by the IdP. Moreover, SP cannot correlate different sessions of the same subject, ensuring a certain level anonymity.

B. Liberty Alliance

The Liberty Alliance Project has emerged in order to create open specifications for the management of federated identities. These specifications were addressed to the integration with Web Services applications. One of the main strengths of this project is its influence on standards such as SAML, whose extensions proposed by Liberty Alliance are now part of SAML 2.0 [6]. The specifications propose the opaque identifiers or pseudonyms, with the aim to ensure the privacy of users. Given each SP, the IdP may assign different pseudonyms to the same user. Thus, the same user may be represented by a different identifier for each service he accesses. It makes it very hard for companies to track user activity based on his transactions.

C. Shibboleth Project

The Shibboleth was developed to be a generic solution to federated Identity, which may be adopted by any type of organization. It is based on open standards such as XML and SAML and provides an easy way to enable applications to use facilities of a federated identity model such as, for example, the concept of SSO and secure exchange of user attributes for SPs that take part of a Shibboleth federation. Several functionalities not specified on SAML 1.x were implemented in Shibboleth in order to provide SSO. Most of these features were incorporated by SAML 2.0 and current versions of Shibboleth (starting from 1.3) are fully compliant implementations of several SAML profiles. Shibboleth has an emphasis on the privacy of users' attributes. The release of these attributes for SPs is restricted by the privacy policy of the origin domain and also by user preferences. There are three main roles within a Shibboleth domain:

- IdP and SP – the first is responsible for authenticating their users before they can make use of the services offered by the second. In Shibboleth, the authentication process is always performed at origin domain of the user, through his IdP, making use of authentication mechanisms present in his organization (or domain). The authentication of users can be done through username and password, Kerberos, X.509, etc. Although most of the time both IdP and SP implement the entire software stack provided by the Shibboleth project, it is possible to use other solutions that are compliant with SAML 2.0.
This allows user credentials to be transported from the IdP to SPs.

- Discovery Service (DS) also called “Where Are You From?” (WAYF) is an additional component that allows the user to choose an IdP in multi-domain architecture of identity. The WAYF can be used by the SP to determine the user's preferred IdP with or without user interaction.

D. The Web Services Framework (WS-)*

This approach is a set of specifications that extend the basic Web services protocol stack with additional security features, to improve the interoperability of different information systems across the Internet. The features of WS-Security are extended by the specifications (WS-Policy, WS-Trust and WS-Privacy). The overall structure of the WS-* architecture is presented in “Fig. 5”.

- *WS-Trust:* specification introduces a protocol for exchanging security credentials among different security domains and also provides means for checking whether a credential can be trusted or not, so that user and SPs evolved in interactions can detect and extend trust relationships based on the credential emission and validity checks. The trust model defined in WS-Trust is based on the Security Token Service (STS). The STS is a Web Service that implements a standard WSDL interface, where operations for the emission, renewal, validation and revocation of credentials are defined. Thus, the STS serve as a trust mediator between the different security domains. The STS are quite general messages to exchange and allow extensions and future compositions. Each operation specifies which XML elements should be included in the corresponding message. The general message of request includes the RST (RequestSecurityToken) contains general parameters like request type, service requirements, the credential type, etc. Depending on the type of request, it may contain more specific elements, such as proof of possession of a private key, expiration date of the tokens, etc. The RSTR (RequestSecurityTokenResponse) contains basically the requested token along with credential parameters (type, expiration date, usage context, etc.).

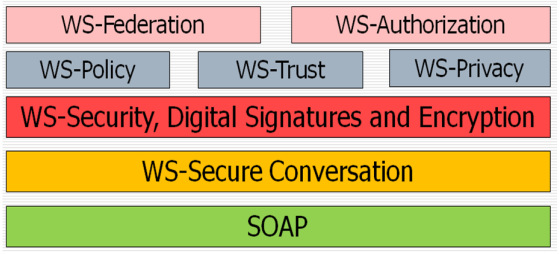

Figure 5. Components of Web Services Security Framework

- *WS-Federation:* is a specification that defines mechanisms based on the WS-* standards (WS-Trust, WS-Security, WS-Policy…), for the construction of federations. These standards already define the basis for managing federated identities, but the WS-Federation proposes extensions that define how to combine these models in order to provide richer functionality to the security domains (or administrative domains) in and across federations.

E. OpenID

OpenID[2] is framework that is lightweight, scalable and extensible. It is based on Web standards like HTTP and URIs, provides User-Centric model and SSO authentication. The basic idea is that a user may access a Web site if he is able to demonstrate that he controls an OpenID identifier.
This identifier is usually a URL (Uniform Resource Locator) or, in some cases, an XRI (Extensible Resource Identifier). Nowadays, many organizations and providers are using OpenID authentication to provide access to their Web sites. The OpenID version 2.0 adopts User-Centered model and implements the concept of federated identity.
The latest OpenID specifications are composed of the following modules:

- *Authentication 2.0* – defines the basic authentication framework including the format and flow of messages between the components of the infrastructure. This module also defines the core set of concepts which are integrated by the framework:
  - ✓ *End User* – represents the user (or person).
  - ✓ *Relying Party (RP)* – The web site that the user is performing accesses using his OpenID identifier.
  - ✓ *Identifier* – refers to a URL (or a URI) which represents the end user's digital identity;
  - ✓ *Claimed Identifier* – an identifier which has not been verified by the Consumer and "claimed" by the user is noted as claimed identifier.
  - ✓ *Verified Identifier* – an identifier is "verified" when the user proves to Consumer, using some method of authentication, that he is the owner of the identifier.
  - ✓ *Identity Provider* – an OpenID Provider (OP) is the server where users' credentials are stored. An OpenID URI of a user refers to the IdP (the server) where the credential is stored;
  - ✓ *User Agent* – represents the end user's Web browser.
- *Attribute Exchange 1.0* – defines how authentication messages can be extended to include additional information (attributes) about users.
- *Provider Authentication Policy Extension 1.0* – allows IdPs to describe security properties of the mechanisms employed in order to verify the user identity.
- *Simple Registration Extension 1.0* – defines a small set of attributes commonly used by SPs for user registration (e.g. full name, e-mail address, date of birth and preferred language);
- *Yadis Discovery Protocol* – used to discover the OpenID Provider given the use URL identifier.

- *OpenID Operation*

OpenID operation is based around an authentication protocol where OP issue assertions that prove a user owns a given identifier. Such assertions are consumed by SPs in order to give the user access to services. OpenID authentication protocol specifies the message exchanges used in order to fulfill the authentication process. The protocol overview is shown in "Fig. 6" and described below:

[2] OpenID : http://openid.net/

1. The user starts the authentication process presenting an identifier to the RP (the Web site which the user wants to access and that supports OpenID login);

2. Based on the identifier provided by the user, the RP performs the discovery of the URL of the OP that will authenticate the user;

3. (Optional) An association is created between RP and OP. The association's secret key is established using the Diffie-Hellman protocol for key exchanges. This association is created to enable verification of messages exchanged between OP and RP;

4. The RP redirects the user's browser to the OP with an OpenID authentication request;

5. The OP verifies if the end user is registered and associated to the informed identifier. The specification does not describe the way in which OPs should authenticate end users: each OP is free for choosing the most appropriate way to perform user authentication and to ensure that he is the identifier owner. For example, Google uses the Google Account password;

6. After the authentication, the OP redirects the end user's browser back to the RP passing an assertion indicating that the user was identified (positive assertion) or the authentication failed (negative assertion);

7. The RP verifies the information sent by the OP, which includes also the checking of the returned URL, the discovered information (OP), the nonce and signature. The verification can be done through the signature included in the message, in case there is an association between OP and Consumer. In case an association is not available, the Consumer may send a request directly to the OP for verification.

This process is carried out whenever the End User tries to access an OpenID enabled Consumer. If the user presents the same identifier in a subsequent access to a different Consumer, the Steps 1 to 4 of the protocol are executed in exactly the same way as in the first authentication. The Step 5, in the other hand, may happen differently: if the OpenID provider initiates a session with the End User after the first authentication, this session is used in order to avoid the user to authenticate again. In this case, Step 5 occurs transparently to the End User and the protocol continues as in the first authentication. This mechanism is the Single Sign-On facility provided by OpenID (notice that step 5 is not specified, so SSO is not a requirement of OpenID, but it is easily implemented and generally adopted).

This architecture largely directed at sharing users' information could be a challenge to maintain the information privacy. For minimizing this problem, the OpenID 2.0 allows logins with the use of pseudonyms and the OP has some facilities for knowing all RPs which the user has visited.

- *Attribute Exchange Extension*

This specification defines messages that can be used by Consumers to request access to attributes of the End User stored in the OP. The attribute fetch and store requests are embedded in OpenID standard authentication requests in a way to leverage the security mechanisms provided by such exchanges. The attribute fetch request contains a list of attributes that are to be read from the OP. Besides, the Consumer may indicate what attributes are required in order for the service to be provided to the End User. The Consumer requirements

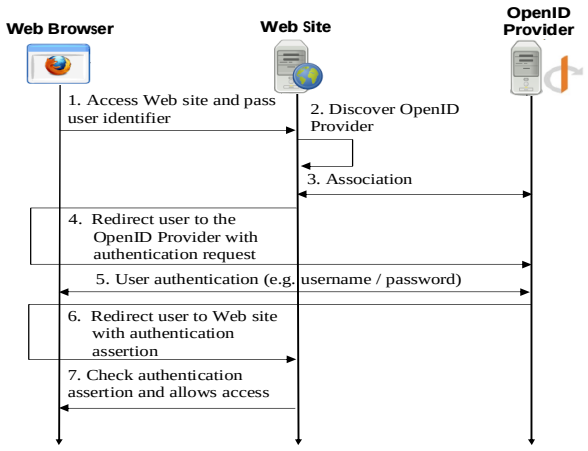

Figure 6. Interactions in OpenID Authentication

are just a hint and the OP is free to decide which attributes it should release (possibly conforming to the End User policies). The response of an attribute fetch request contains a list of attribute values conforming to the Consumer's request and the internal attribute release policy of the OP.
Besides attribute requests, the OpenID Simple Registration Extension defines a simplified protocol of attribute exchange in which the Consumer requests a small set of predefined attributes commonly employed in user registration. These attributes are exchanged in the same way as the attribute exchange requests so they are subject to the same security considerations.

F. OAuth

OAuth (RFC 5849 2007) allows a user to access resources located on another site without disclosing its identifiers/passwords. A third party site acts on behalf of the user. OAuth version 2.0 is not backward compatible with OAuth 1.0. OAuth 2.0 is open to the domain of business and Cloud, enabling and incorporating specific use cases that make it suitable for authentication and authorization with REST API (REpresentational State Transfer). OAuth is becoming widespread in the web authentication domain. One of the strengths of the system is the simplicity with which the information is centralized and authenticated.

G. Higgins Project of the Eclipse Foundation

The initial motivation for the Higgins[3] project was to implement an IdM based on the User-Centric model. This framework aims to allow users to have more control, convenience and privacy over their identity and profile information. User should be able to decide what information to be shared and with which websites.
The identities of the Higgins model follows the approach based on active client (identity selector), i.e., an application needs to help user for controlling his multiple identities and preferences. Higgins offers users three applications that act as identity selectors for the creation, selection, management and sharing of i-cards which represent user's identities in different contexts and relationships.
In this model, it is also possible to cross contexts and manage any type of user information such as favorite songs, driving license number, social insurance number and health plan among others, stored on a card. In Higgins model, selectors are interoperable with CardSpace. These selectors of identities are available for some operating systems (Mac OSX, Linux and Windows) as well as browsers Firefox and Internet Explorer.

H. CardSpace (InfoCard)

The challenge is to create, use and manage the identity diversity in a meaningful way. The system CardSpace, is a platform component of Microsoft.Net designed to offer users a consistent support for handling with multiple digital identities. Microsoft has documented the protocol implemented by Cardspace in the InfoCard[4] specification. Furthermore, it is also supported in the browser Internet Explorer (since version 7.0). The Cardspace focuses on user data collections called information cards, presented in a software interface, named identity selector (similar to a wallet with cards identifying the user). Each InfoCard represents a different identity. When a SP requests user credentials, the user agent picks from the selector program, one of their identities.

V. COMPARISON BETWEEN THE DIFFERENT AAIS

This section analyzes and compares infrastructures and technologies used for building an IdM. This overview is not intended to draw up an exhaustive list of all IdM infrastructures. The diversity of specifications and the terminologies used in the various infrastructures make the comparison of these IAAs very difficult.

A. Considerations about AAIs solutions

The AAIs described in section IV share some points in common, such as SSO, distribution of authentication procedures, attributes exchange, concerns about user privacy and anonymity.
The SAML specifications present a general framework for dealing with federated identities, in which metadata are defined to represent security information, protocols for exchanging security assertions and trust relations. It was employed by several other IdM solutions. There is some overlap between WS-Federation and SAML standards. Both solutions allow federated IdM and provide a similar set of features. WS-Federation provides SSO, Single Logout, attributes exchange (based on privacy policies), trusted relationships, permanent and transient pseudonyms and metadata documents. The main difference is that the

[3] http://www.eclipse.org/higgins/
[4] http://msdn.microsoft.com/en-us/library/aa480189.aspx

WS-Federation is based on the trust model of WS-Trust and allows the use of any credentials, not only SAML assertions.
The Liberty Alliance project aimed to facilitate business interactions, taking advantage of Service Oriented Architecture (SOA) and the concept of federation, which is characterized by the notion of circles of trust in the specifications. One of the contributions of this project was having influenced SAML specifications, many suggestions of Liberty Alliance are now part of SAML 2.0. The Liberty Alliance project provides similar features to those of WS-Federation which is founded on a stack of all Web services specifications such as WS-Trust and WS-Policy.
The Shibboleth project is based on open standards (XML, SAML), it inherits their features and provides an easy way to enable applications to use facilities of a federated identity model. Several functionalities specified in SAML 2.0 were implemented in Shibboleth in order to provide the SSO and secure exchange of user attributes for all SPs that take part of a Shibboleth federation.
OpenID, CardSpace and Higgins are frameworks that support IdM approaches of federated identities and User-Centric controls. Among these infrastructures, the best succeeded is OpenID. It has been widely used, especially due to partnership with companies offering Web 2.0 applications. One advantage of OpenID is that it does not require software on the client side. OpenID approach adopts the identity model based on address. This identifier is usually a URL or, in some cases, an XRI. CardSpace and Higgins adopt the model of active client (with Identity Selector) and identity approaches based on cards (tokens). The active client of Higgins is available for different platforms of data representation and accepts all well-known protocols to digital identities, including WS-Trust, OpenID, SAML, XDI, LDAP, and others. The literature shows that Higgins approach is considered more flexible because it supports identities provided from different sources and prevents an IdP of tracking the SPs (applications) accessed by the user. While providing support for any type of security token, the protocols adopted in CardSpace only follow WS-* standards, focusing mainly on WS-Trust. However, project Higgins follows a more independent solution, since it supports IdPs based on WS-Trust but also based on SAML 2.0.
OAuth comes from the social web; it is an open protocol that supplies a standard API for user authentication in desktop and Web applications. The main goal of OAuth is to allow an application to be authenticated to another "on behalf of a user" without needing access to his password. It defines mechanisms for granting user accesses to resources. OpenID and OAuth can work together.
SAML is considered an open identity technology, but its previous need for trust relationships between IdPs and SPs, makes this technology not scalable to Web 2.0 applications. Given this, open trust frameworks are being developed to enable the Government websites and applications to accept credentials issued by different IdPs, commercial and academic.

B. Considerations about Privacy in IAAs

The privacy is of paramount importance, any infrastructure of IdM must adequately protect user information and must adhere to the privacy policies defined to the user personal data. It is necessary to take into account that federated IdM becomes a crucial task in large systems and also the multiples threats against privacy of user data. Federated identity systems often manipulate different kinds of identifiers in different contexts. Such identifiers can have an absolute meaning (context independent) or relative (context dependent) [7]. The privacy in federations may be emphasized with minimal data disclosure. For example, authentications and authorizations can be performed with LoA and a minimal data disclosure by providing only identifiers and attributes necessary to ensure the service execution or resource accesses.
An important technique for the preservation of privacy is the use of pseudonyms, which are user identifiers that do not allow inferences regarding the real identity, properties, or attributes of users to whom they refer.
WS-Federation defines a Pseudonyms Service which is responsible for associating pseudonyms to user identities. In WS-Federation, pseudonym may have different levels of volatility allowing different levels of customization and privacy. For example, a subject can have pseudonyms which last only one authentication session. In addition to increase its privacy, it prevents services to associate any persistent information with the subject (preventing customization). Unlike IdP and Attribute Service, the Pseudonym Service uses a different interface not based on the STS, but defined in the WS-Transfer. This specification defines methods to create, delete, update and access existing pseudonyms.
The pseudonyms which are used in SAML Assertions are built based on pseudo-random values that do not have discernible correlation with user identifiers in IdPs or SPs. A pseudonym has a meaning only in the context of the relationship between the two communicating parties. Pseudonyms are also intended to difficult the association between users and their transactions (services being accessed).

Specifications of Liberty Alliance also address issues about policies of privacy multi-level, which make use of privacy labels similar to privacy and security labels in Mandatory Access Control (MAC). In MAC controls, each resource is tagged with a security label that represents the sensitivity of the resource considered. A user (subject) wishing to access a resource must have an authorization level (clearance level) appropriate to the security label of the resource. In these specifications, privacy levels follows the privacy policies available in the IdPs (which also serve like repositories for user attributes) and are assigned to user data and to attribute requests sent by SPs to IdPs.
In Shibboleth, the release of users' attributes for SPs is conditioned by the privacy policy of the origin domain and also by user preferences. The great limitation of CardSpace and Shibboleth is that the user can select only one IdP and submit only one credential to a SP. For solving this problem, it is proposed a component called Linking Service [8]. The idea of this service is to allow users to add various attributes from different IdP and yet preserving the privacy of those users.
The Higgins project also intends to work this problem, but the current version does not yet offer a solution.

C. Levels of Assurance in IdM IAAs

In OAuth or OpenId, when generating user accounts, the IdP does not have means to confirm the user's real identity. In this case, the LoA of the Identity is low. OpenID is currently used mostly for low-risk applications like blogs and social networking, not commerce, education, or government.
The SAML allows to associate quality levels to its authentication assertions, providing, in this way, a standard way to define levels of information exchange between IdP and SP. Therefore, LoA can be included in Authentication Context (*AuthnContext*) mechanisms for providing a simplified way of representing a LoA authentication scheme and to enable the authentication service to include some information related to the quality of the authentication process.
According to the E-Authentication Federation rules (EAF), the LoA value is a compulsory attribute that must be present whenever a SAML authentication assertion is issued. The EAF has defined a special URI, to uniquely identify the LoA attributes, and the attribute can only have values of 1, 2, 3, 4 or "test".
Like SAML, Liberty Alliance formed the Identity Assurance Expert Group (IAEG). The IAEG's objective is to create a framework of baseline policies, business rules, and commercial terms against which IdPs can be assessed and evaluated. The primary deliverable of IAEG is the Liberty Identity Assurance Framework (LIAF). Which goal is to facilitate identity federation to promote uniformity and interoperability amongst IdPs, with a specific focus on the level of trust (LoT), or LoA, associated with Identity Assertions.
WS-Trust specification defines the *(AuthenticationType)* parameter to indicate an authentication type that is required (or performed) with respect to a particular security token request. However, there are no specific recommendations regarding mechanism or LoA and no particular types are defined or required. To facilitate interoperability WS-Federation has defined a set of URIs for specifying common authentication types and LoA that can be used for the wst : (*AuthenticationType)* parameter in RST and RSTR messages.
CardSpace and Higgins are two Identity Metasystems, entirely agnostic about the format of the security token that's requested from an IdP and passed on to a SP. Both identity systems are built around the abstraction of the information card, which is a standard representation of the user information.
In fact, CardSpace and Higgins typically aren't even aware of what format is in this token. Because of this, these systems can work with any digital identity system, using any type of security token. Basically, in these systems, when the user tries to access some service, the information card client installed in his device recovers the SP policy to determine the requirements of the service. The user selects one of the cards satisfying the policy requirements; the information card application contacts the IdP that issued that card to get a signed token. Finally, this signed token is sent to the SP for authorizing access to the aimed service. The required LoA for getting access to the service depends on the SP policy and the authentication requirements defined for this service. The use of the SP policy in these systems provides the same assurance level that is described in SAML or Liberty Alliance infrastructures.

VI. Conclusions And Final Considerations

The current technologies are offering new possibilities of connections. However, the way people and organizations (private and public) will make use of these opportunities and applications will depend on the progress of digital identity authentication [9]. Unfortunately, the use of the infrastructures for IdM can be a deterrent, analyzing costs vs. benefits. Even on the assumption that the trusts relationships are already pre-

established. Yet there are several challenges to implement authentication credentials on a federation. SPs and domains have the autonomy to decide which policies and security technologies they want to use.
The latest solutions have also emphasized User-Centric models. In particular OpenID and CardSpace has attracted a lot of interest, especially of SPs that follow Web 2.0 approach and by governments who wish to actively include people in their social networks and E-Gov programs.
Through our investigation, we identified a significant interest across various communities, in using Levels of Assurance and levels of Trust as a means to refine access control to sensitive resources and to evaluate the authentication process. This may enable SPs to make their access control decisions based on the LoT and to link the LoA with authorization decisions, helping to mitigate risks and provide more secure and fine-grained access control. The main frameworks and models of IdM were described and analyzed in this text. It was indicated the importance of SAML 2.0. SAML based infrastructures are strong candidates to be adopted for identity management in the context of SecFuNet project. They present several interesting features.
The interoperability guaranteed by the use of SAML is effective and well accepted. SAML assertions allow the use of many different authentication technologies, making these frameworks very interesting for heterogeneous environments.
Despite the indicated advantages, there are limitations in order to fulfill the SecFuNet requirements. In particular, the support for SmartCards is either limited or non-existent and even I-Cards are not an option. Besides, these infrastructures are based in complex protocols that require the inclusion of large implementation stacks in clients limiting the utilization of these infrastructures in mobile devices.
Despite the gap in supporting LoA (low level) and privacy protection, we concluded that the most effective platform to fulfill, at least in part, the SecFuNet requirements is OpenID. Indeed, the protocols for authentication and attribute exchanges are extremely simple in this Framework; it easily integrates in a wide variety of applications and devices. OpenID may be used with any kind of authentication technology.
To increase LoA and LoT levels of OpenID, to effectively manage SSO and users attributes, we can combine different solutions with OpenID. In particular, the User-Centric identity, this will be implemented in the SecFuNet project.
Effectively, we are planning to introduce smart cards and user controls in attributes' delivery in the OpenId. So, we are extending this infrastructure for supporting authentication mechanisms based on LoA and LoT.

REFERENCES

[1] D. W. Chadwick, "Federated IdM," Foundations of Security Analysis and Design V, 2009, pp. 96–120.
[2] A. Bhargav-Spantzel, J. Camenisch, T. Gross and D. Sommer, "User centricity: a taxonomy and open issues," Journal of Computer Security, October 2007, Vol 15 Issue 5, pp. 493-527.
[3] T.E. Maliki, and J-M. Seigneur, "A survey of user-centric identity management technologies," The International Conference on Emerging Security Information, Systems, and Technologies, SecureWare, October. 2007, pp 12–17.
[4] J. Camenisch, and B. Pfitzmann, "Security, Privacy, and Trust in Modern Data Management," Chapter "Federated Identity Management," Springer Verlag, 2007, pp 213–238.
[5] E. Maler, and D. Reed, "The venn of identity: Options and issues in federated IdM," IEEE Security & Privacy, April 2008, Vol 6, Issue: 2, pp. 16–23.
[6] R. Baldoni, "Federated Identity Management Systems in e-Government: the Case of Italy. Electronic Government," Electronic Government, an International Journal, 2012, Vol.9, No.1, pp.64-84.
[7] G. J. Ahn, and J. Lam, "Managing privacy preferences for federated identity management," ACM-DL, DIM '05: Proceedings of the 2005 workshop on Digital identity management, 2005, pp. 28–36.
[8] D. W. Chadwick, and G. Inman, "Attribute Aggregation in Federated Identity Management," IEEE Computer Society, May 2009, Vol 42, Issue 5, pp. 44–53.
[9] J. A. Lewis, (2008). "Authentication 2.0 - new opportunities for online identification," Technical report, Center for Strategic and International Studies, January 2008.